## Commutative algebra draught

NOETHERIAN RINGS. We write $(f_1, f_2, \dots, f_m)$ for the ideal $\{g_1 f_1 + g_2 f_2 + \cdots + g_m f_m \mid g_\nu \in A\}$ spanned (as $A$-module) by $\{f_1, f_2, \dots, f_m\} \subset A$. A commutative ring $A$ is called *Noetherian*, if it satisfies the next lemma:

Lemma 8.1. *The following properties of a commutative ring $A$ are mutually equivalent*

1) *any set of elements $f_\nu$ contains some finite subset that generates the same ideal as the initial set;*
2) *any ideal admits a finite set of generators;*
3) *for any infinite chain of embedded ideals $I_1 \subset I_2 \subset I_3 \subset \cdots$ there exists $n \in \mathbb{N}$ such that $I_\nu = I_n \quad \forall\, \nu \geqslant n$.*

Proof. Clearly, (1) $\Rightarrow$ (2). To deduce (3) from (2), take a finite set of generators for the ideal $I = \bigcup I_\nu$; since they belong to some $I_n$, we have $I_\nu = I_n = I \ \forall\ \nu \geqslant n$. Finally, (1) follows from (3) applied to the chain $I_n = (f_1, f_2, \dots, f_n)$, where $f_i$ are chosen from $\{f_\nu\}$ in order to have $f_\nu \notin (f_1, f_2, \dots, f_{\nu-1})$. □

Theorem 8.2. (Hilbert's base theorem). *If $A$ is Noetherian, then $A[x]$ is Noetherian too.*

Proof. Let $I \subset A[x]$ be an ideal. We write $L_d \subset A$ for a set of leading coefficients of all degree $d$ polynomials in $I$. Clearly, each $L_d$ and $L_\infty \stackrel{\text{def}}{=} \bigcup_d L_d$ are ideals in $A$. Let $L_\infty$ be generated by $a_1, a_2, \dots, a_s \in A$ coming from $f_1^{(\infty)}, f_2^{(\infty)}, \dots, f_{s_\infty}^{(\infty)} \in I$ and let $\max_\nu(\deg f_\nu) = m$. Similarly, write $f_1^{(k)}, f_2^{(k)}, \dots, f_{s_k}^{(k)}$ for the polynomials whose leading coefficients span the ideal $L_k$ for $0 \leqslant k \leqslant m-1$. To finish the proof, make: □

Exercice 8.3. Show that $I$ is spanned by $s_0 + \cdots + s_{m-1} + s_\infty$ polynomials $f_\nu^{(\mu)}$ just constructed.

Corollary 8.4. *A polynomial ring $A[x_1, x_2, \dots, x_n]$ over a Noetherian ring $A$ is Noetherian as well.* □

Corollary 8.5. *Any finitely generated $k$-algebra is Noetherian for any field $k$.*

Proof. A polynomial algebra $k[x_1, x_2, \dots, x_n]$ is Noetherian by the previous corollary. Any its factor algebra $A$ is Noetherian as well: full preimage of any ideal $I \subset A$ under the factorizing morphism $k[x_1, x_2, \dots, x_n] \twoheadrightarrow A$ is an ideal in $k[x_1, x_2, \dots, x_n]$, i. e. admits a finite set of generators, whose classes span $I$ over $A$, certainly. □

INTEGRALITY. Let $A \subset B$ be two commutative rings. An element $b \in B$ is called *integer* over $A$, if it satisfies the conditions from Lemma 8.6 below. If all $b \in B$ are integer over $A$, then $B$ is called an *integer extension* of $A$ or an *integer $A$-algebra*.

Lemma 8.6. *The following properties of an element $b \in B$ are pairwise equivalent:*

1) *$b^m = a_1 b^{m-1} + \cdots + a_{m-1} b + a_0$ for some $m \in \mathbb{N}$ and some $a_1, a_2, \dots, a_m \in A$;*
2) *$A$-module spanned by all nonnegative powers $\{b^i\}_{i \geqslant 0}$ admits a finite set of generators;*
3) *there exist a finitely generated faithful[1] $A$-submodule $M \subset B$ such that $bM \subset M$.*

Proof. The implications (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3) are trivial. To deduce (1) from (3), let $\{e_1, e_2, \dots, e_m\}$ generate $M$ over $A$ and let the multiplication $M \xrightarrow{m \mapsto bm} M$ be presented by a matrix $Y$, i. e. write $(be_1, be_2, \dots, be_m) = (e_1, e_2, \dots, e_m) \cdot Y$.

Note that if $A$-linear map $M \xrightarrow{\varkappa} M$ takes $(e_1, e_2, \dots, e_m) \longmapsto (e_1, e_2, \dots, e_m) \cdot X$, where $X$ is a square matrix with entries in $A$, then there is an inclusion $(\det X) \cdot M \subset \operatorname{im} \varkappa$, which follows from the Laplace identity $\det X \cdot \mathrm{Id} = \widehat{X} \cdot X$ applied to $(e_1, e_2, \dots, e_m)$.

In our case the zero operator $M \xrightarrow{\varkappa} 0$ can be presented by the matrix $X = b \cdot \mathrm{Id} - Y$. So, the multiplication by $\det(b \cdot \mathrm{Id} - Y)$ annihilates $M$. Since $M$ is faithful, $\det(b \cdot \mathrm{Id} - Y) = 0$. This is a polynomial equation on $b$ with the coefficients in $A$ and the leading term $b^n$ as required in (1). □

Example 8.7: Integer algebraic numbers. Let $K \supset \mathbb{Q}$ be a finite dimensional[2] field extension; then elements $z \in K$ are called *algebraic numbers*. Such a number $z$ is integer over $\mathbb{Z}$ iff there are some $\vartheta_1, \vartheta_2, \dots, \vartheta_m \in K$ such that the multiplication by $z$ sends their $\mathbb{Q}$-linear span to itself and is presented there by a matrix whose entries belong to $\mathbb{Z}$.

Example 8.8: Invariants of a finite group action. Let a finite group $\mathfrak{G}$ act on a $k$-algebra $B$ via $k$-algebra automorphisms $B \xrightarrow{g} B$, $g \in \mathfrak{G}$, and let $A = B^{\mathfrak{G}} = \{a \in B \mid ga = a \ \forall g \in \mathfrak{G}\}$ be the subalgebra of $\mathfrak{G}$-invariants. Then $B$ is an integer extension of $A$. Indeed, if $b_1, b_2, \dots, b_s \in B$ form a $\mathfrak{G}$-orbit of any given $b = b_1 \in B$, then the polynomial $\beta(t) = \prod(t - b_i)$ is monic[3], lies in $A[t]$, and annihilates $b$.

[1] $A$-module $M$ is called *faithful*, if $aM = 0$ implies $a = 0$ for $a \in A$

[2] as a vector space over $\mathbb{Q}$

[3] a polynomial is called *monic* or *unitary*, if its leading coefficient equals 1

INTEGER CLOSURES. A set of all $b \in B$ that are integer over a subring $A \subset B$ is called *an integer closure* of $A$ in $B$. If this closure coincides with $A$, then $A$ is called *integrally closed* in $B$.

Lemma 8.9. *The integer closure of $A$ is a subring in $B$ (in particular, $ab$ is integer for any $a \in A$ as soon as $b$ is integer). If $C \supset B$ is an other commutative ring and $c \in C$ is integer over an integer closure of $A$ in $B$, then $c$ is integer over $A$ as well (in particular, any integer $B$-algebra is an integer $A$-algebra as soon as $B$ is an integer $A$-algebra).*

Proof. If $p^m = x_{m-1}\, p^{m-1} + \cdots + x_1\, p + x_0$, $q^n = y_{n-1}\, q^{n-1} + \cdots + y_1\, q + y_0$ for $p, q \in B$, $x_\nu, y_\mu \in A$, then $A$-module spanned by $p^i q^j$ with $0 \leqslant i \leqslant (m-1)$, $0 \leqslant j \leqslant (n-1)$ is faithful (it contains 1) and goes to itself under the multiplication by both $p+q$ and $pq$. Similarly, if $c^r = z_{r-1}\, c^{r-1} + \cdots + z_1\, c + z_0$ and all $z_\nu$ are integer over $A$, then a multiplication by $c$ preserves a faithful $A$-module spanned by a sufficient number of products $c^i z_1^{j_1} z_2^{j_2} \cdots z_r^{j_r}$. □

Corollary 8.10. [4] *For any two commutative rings $A \subset B$ let $f(x), g(x) \in B[x]$ be two monic polynomials. Then all coefficients of $h(x) = f(x)g(x)$ are integer over $A$ iff all coefficients of both $f(x)$, $g(x)$ are integer over $A$.*

Proof. There exists[5] a ring $C \supset B$ such that $f(x) = \prod(t - \alpha_\nu)$ and $g(x) = \prod(t - \beta_\mu)$ in $C[x]$ for some $\alpha_\nu, \beta_\mu \in C$. By Lemma 8.9, all coefficients of $h(x) = \prod(t - \alpha_\nu) \prod(t - \beta_\mu)$ are integer over $A \iff$ all $\alpha_\nu, \beta_\mu$ are integer over $A \iff$ all coefficients of $f(x)$ and $g(x)$ are integer over $A$. □

Lemma 8.11. *Let $B \supset A$ be integer over $A$. If $B$ is a field, then $A$ is a field. Vise versa, if $A$ is a field and there are no zero divisors in $B$, then $B$ is a field.*

Proof. If $B$ is a field integer over $A$, then any non zero $a \in A$ has an inverse $a^{-1} \in B$, which satisfy an equation $a^{-m} = \alpha_1\, a^{1-m} + \cdots + \alpha_{m-1}\, a^{-1} + \alpha_0$ with $\alpha_\nu \in A$. We multiply the both sides by $a^{m-1}$ and get $a^{-1} = \alpha_1 + \cdots + \alpha_{m-1}\, a^{m-2} + \alpha_0\, a^{m-1} \in A$. Conversely, if $A$ is a field and $B$ is an integer $A$-algebra, then all non negative integer powers $b^i$ of any $b \in B$ form a finite dimensional vector space $V$ over $A$. If $b \neq 0$ and there are no zero divisors in $B$, then $x \longmapsto bx$ is an injective linear operator on $V$, that is, an isomorphism. A preimage of $1 \in V$ is $b^{-1}$. □

Example 8.12: algebraic elements and minimal polynomials. If $A = k$ is a field and $B \supset k$ is a $k$-algebra, then $b \in B$ is integer over $k$ iff $b$ satisfy a polynomial equation $f(b) = 0$ for some $f \in k[x]$. Traditionally, such $b$ is called *algebraic* over $k$ rather than *integer*. We write $k[b]$ for a $k$-linear span of nonnegative integer powers $\{b^n\}_{n \geqslant 0}$ and $k(b)$ for a $k$-linear span of all integer powers $\{b^n\}_{n \in \mathbb{Z}}$ (if such exist in $B$). Clearly, $k[b] \subset B$ is the minimal $k$-subalgebra containing 1 and $b$; in other terms, $k[b] = \operatorname{im}(\mathrm{ev}_b) = k[x]/\ker(\mathrm{ev}_b)$, where $\mathrm{ev}_b : k[x] \xrightarrow{f(x) \mapsto f(b)} B$ is *an evaluation homomorphism*. If $b$ is algebraic, then $\ker(\mathrm{ev}_b) = (f) \stackrel{\text{def}}{=} f \cdot k[x]$ for some $0 \neq f \in k[x]$, because $k[x]$ is a principal ideal domain. This $f$ is fixed uniquely as a monic polynomial of lowest degree such that $f(b) = 0$; it is called *the minimal polynomial* of $b$ over $k$. Note that $k[b]$ is a $\deg(f)$-dimensional vector space over $k$ with a basis $1, b, b^2, \ldots, b^{\deg(f)-1}$. If $B$ does not have zero divisors, then $k[b]$ is a field by Lemma 8.11; in particular, the minimal polynomial of $b$ is irreducible in this case. If $b$ is not algebraic, then $\ker(\mathrm{ev}_b) = 0$ and $k[b] \simeq k[x]$ is a polynomial ring. In particular, it is an infinite dimensional vector space over $k$ and it is not a field. This phenomenon will be generalized in Lemma 8.17 below.

Lemma 8.13. *Let $k = Q(A)$ be the fraction field for a commutative ring $A$ without zero divisors, $B$ be any $k$-algebra, and $b \in B$ be algebraic over $k$ with minimal polynomial $f \in k[x]$. If $b$ is integer over $A$, then all coefficients of $f$ are integer over $A$.*

Proof. Since $b$ is integer, $g(q) = 0$ for some monic $g \in A[x]$. Then $g = fh$ in $k[x]$ for some monic $h \in k[x]$ and all the coefficients of $g$, $h$ are integer over $A$ by Corollary 8.10. □

NORMAL RINGS. A commutative ring $A$ without zero divisors is called *normal*, if there are no $b \in Q(A) \setminus A$ integer over $A$. Certainly, any field is normal.

Exercice 8.14. Show that the ring $\mathbb{Z}$ is normal.

HINT. A polynomial $a_0 t^m + a_1 t^{m-1} + \cdots + a_{m-1} t + a_m \in \mathbb{Z}[t]$ annihilates a fraction $p/q \in \mathbb{Q}$ with coprime $p, q \in \mathbb{Z}$ only if $q | a_0$ and $p | a_m$

Corollary 8.15. *Let $A$ be a normal ring and $f \in A[x]$ be factorized in $Q(A)[x]$ as $f = g\,h$. If both $g$, $h$ are monic, then necessarily $g, h \in A[x]$.*

Proof. Indeed, all the coefficients of $g, h$ are integer over $A$ by Corollary 8.10. □

Corollary 8.16. *Let $A$ be normal ring with the fraction field $k = Q(A)$ and $B$ be any $k$-algebra. Then $b \in B$ is integer over $A$ iff it is algebraic over $k$ and its minimal polynomial (over $k$) lies in $A[x]$.*

Proof. This follows immediately from Lemma 8.13. □

[4] it is known as Gauss - Kronecker - Dedekind lemma

[5] For any commutative ring $A$ and any monic non constant $f(x) \in A[x]$ there exists a commutative ring $C \supset A$ such that $f(x) = \prod(x - c_\nu)$ in $C[x]$ for some $c_\nu \in C$. It is constructed inductively as follows. Consider a factor ring $B = A[x]/(f)$ (which contains $A$ as the congruence classes of constants) and put $b \stackrel{\text{def}}{=} x \pmod f \in B$. Then $f(b) = 0$ in $B[x]$. Hence the residue after dividing $f(x)$ by $(x - b)$ in $B[x]$ vanishes and we get the factorization $f(x) = (x - b)h(x)$ with $h(x) \in B[x]$. Now repeat the procedure for $h$, $B$ instead of $f$, $A$ e. t. c.

FINITELY GENERATED COMMUTATIVE $k$-ALGEBRAS. Let $k$ be any field. A commutative $k$-algebra $B$ is called *finitely generated*, if there is a $k$-algebra epimorphism $k[x_1, x_2, \dots, x_m] \xrightarrow{\pi} B$. Images $b_i = \pi(x_i) \in B$ are called *algebra generators* for $B$ over $k$.

Lemma 8.17. *A finitely generated $k$-algebra $B$ is a field only if each $b \in B$ is algebraic over $k$.*

Proof. Let $B$ be generated by $\{b_1, b_2, \dots, b_m\}$. We use induction over $m$. The base case: $m = 1$, $B = k[b]$, was considered in Example 8.12. Let $m > 1$. If $b_m$ is algebraic over $k$, then $k[b_m]$ is a field and $B$ is algebraic over $k[b_m]$ by the inductive assumption. Hence, by Lemma 8.9, $B$ is algebraic over $k$ as well.

So, we only have to show that $b_m$ *must* be algebraic over $k$. Suppose the contrary: let $b_m$ be not algebraic, that is $k(b_m)$ be isomorphic to the field $k(x)$, of rational functions in 1 variable, via sending $b_m \longmapsto x$. Then, by the inductive assumption, $B$ is algebraic over $k(b_m)$ and each of $b_1, b_2, \dots, b_{m-1}$ satisfies a polynomial equation with coefficients in $k(b_m)$. Multiplying these equations by appropriate polynomials in $b_m$, we can put their coefficients into $k[b_m]$ and make all their leading coefficients to be equal to the same polynomial, which we denote by $p(b_m) \in k[b_m]$.

Now, $B$ is integer over the subalgebra $F \subset B$ generated over $k$ by $b_m$ and $q = 1/p(b_m)$. By Lemma 8.11, $F$ is a field. So, there exists a polynomial $g \in k[x_1, x_2]$ such that $g(b_m, q)$ is inverse to $1 + q$ in $F$. Let us write the rational function $g(x\,,\, 1/p(x)) \in k(x)$ as $h(x)/p^k(x)$, where $h \in k[x]$ is coprime to $p \in k[x]$. Multiplying the both sides of

$$\left(1 + \frac{1}{p(b_m)}\right) \frac{h(b_m)}{p^k(b_m)} = 1$$

by $p^{k+1}(b_m)$, we get for $b_m$ a polynomial equation $h(b_m)\,(p(b_m)+1) = p^{k+1}(b_m)$, which is nontrivial, because $h(x)(1+p(x))$ is not divisible by $p(x)$. Hence, $b_m$ should be algebraic over $k$. □

HILBERT'S NULLSTELLENSATZ. Let us write $V(I) = \{a \in \mathbb{A}_n \mid f(a) = 0 \quad \forall\, f \in I\ \} \subset \mathbb{A}^n$ for affine algebraic variety defined by a system of polynomial equations[6] $I \subset k[x_1, x_2, \dots, x_n]$. Vise versa, for any subset $V \subset \mathbb{A}^n$ we write $I(V) = \{f \in k[x_1, x_2, \dots, x_n] \mid f|_V \equiv 0\}$ for a set of all polynomials vanishing along $V$. Clearly, $I(V)$ is always an ideal and $I(V(I)) \supset I$ for any ideal $I$. In general, then last inclusion is proper. For example, if $I = (x^2) \in \mathbb{C}[x]$, then $V(I) = \{0\} \subset \mathbb{A}^1(\mathbb{C})$ and $I(V(I)) = (x)$.

Theorem 8.18. (week Nullstellensatz). *If $k$ is algebraically closed, then $V(I) = \varnothing \iff 1 \in I$ for an ideal $I$.*

Proof. We only have to find a point $p \in \mathbb{A}_n$ such that $f(p) = 0$ for any polynomial $f$ from a given proper ideal $I \subset k[x_1, x_2, \dots, x_n]$. Moreover, it is enough to suppose that $I$ is *maximal*, that is, any $f \notin I$ is invertible modulo $I$. Indeed, otherwise an ideal $J$ generated by $f$ and $I$ would be proper and strictly larger than $I$, i. e. we could replace $I$ by $J$; a finite chain of such replacements leads to some maximal ideal. As soon as $I$ is maximal, the factor algebra $K = k[x_1, x_2, \dots, x_n]/I$ is a field. Hence, any element of $K$ is algebraic over $k \subset K$ by Lemma 8.17. Since $k$ is algebraically closed, this means that any polynomial is (mod $I$)-congruent to some constant. Let $\vartheta_1, \vartheta_2, \dots, \vartheta_n$ be the constants presenting the basic linear forms $x_1, x_2, \dots, x_n \pmod I$. Then any polynomial $f \in k[x_1, x_2, \dots, x_n]$ is (mod $I$) congruent to $f(\vartheta_1, \vartheta_2, \dots, \vartheta_n) \in k$. In particular, $f(\vartheta_1, \vartheta_2, \dots, \vartheta_n) = 0$ for any $f \in I$ as required. □

Corollary 8.19. (strong Nullstellensatz). *Under conditions of Theorem 8.18, $f \in I(V(I)) \iff \exists\, k \in \mathbb{N} : f^k \in I$.*

Proof. Only the implication '$\Rightarrow$' for *nonempty* $V(I) \subset \mathbb{A}^n$ is nontrivial. To prove it, we identify $\mathbb{A}^n$ with the hyperplane $t = 0$ in $\mathbb{A}^{n+1}$ coordinated by $(t,\ x_1, x_2, \dots, x_n\ )$. If $f \in k[x_1, x_2, \dots, x_n] \subset k[t,\ x_1, x_2, \dots, x_n\ ]$ vanishes along $V(I)$, then an ideal $J \subset k[t,\ x_1, x_2, \dots, x_n\ ]$ spanned by $I$ and a polynomial $g(t, x) = 1 - t\,f(x)$ has empty zero set $V(J) \subset \mathbb{A}^{n+1}$, because of $g(x, t) \equiv 1$ on $V(I)$. So, $1 \in J$, i. e. $\exists\quad q_0, q_1, \dots, q_s\ \subset k[t,\ x_1, x_2, \dots, x_n\ ],\quad f_1, f_2, \dots, f_s\ \subset I$ : $q_0(x,t)(1-tf(x)) + q_1(t,x)f_1(x) + \dots + q_s(x,t)f_s(x) = 1$. Then a homomorphism $k[t,\ x_1, x_2, \dots, x_n] \longrightarrow k(x_1, x_2, \dots, x_n)$ sending $t \longmapsto 1/f(x)$, $x_\nu \longmapsto x_\nu$ takes this equality to $q_1(1/f(x)\,,\ x)\,f_1(x) + \dots + q_s(1/f(x)\,,\ x)\,f_s(x) = 1$. Since $I$ is proper, some of $q_\nu(1/f(x), x)$ should have nontrivial denominators. Hence, multiplication by appropriate power $f^k$ leads to an expression we are looking for: $\widetilde{q}_1(x)\,f_1(x) + \dots + \widetilde{q}_s(x)\,f_s(x) = f^k(x)$, where $\widetilde{q}_\nu \in k[x_1, x_2, \dots, x_n]$. □

FACTORIZATION. Let $A$ be a commutative ring without zero divisors. An element $q \in A$ is called *irreducible*, if it is not invertible and $q = rs \Longrightarrow$ one of $r, s$ is invertible. An element $p \in A$ is called *prime* if it generates a prime ideal in $A$, i. e. $A/(p)$ is not zero and does not have zero divisors. In other words, $p$ is prime, if it is not invertible and $p|rs \Longrightarrow p$ divides at least one of $r, s$.

Exercice 8.20. Check that each prime element is irreducible.

A ring $A$ is called *factorial*, if any $a \in A$ is a finite product of irreducible elements $a = q_1\, q_2 \cdots q_m$ and these irreducible factors are defined by $a$ uniquely up to multiplication by invertible elements, i. e. any two irreducible factorizations $q_1\, q_2 \cdots q_m = a = q'_1\, q'_2 \cdots q'_n$ have $m = n$ and (after appropriate renumbering) $q_i = s_i\, q'_i$ for all $i$ and some invertible[7] $s_i \in A$.

Claim 8.21. *Any factorial ring $A$ is normal.*

[6] certainly, we can always extend $I$ to an ideal spanned by $I$ — this does not effect on $V(I)$

[7] if $a = bs$ for an invertible $s$, then $a$ and $b$ are called *associated* (with each other) elements of ring

Proof. Let $\alpha/\beta \in Q(A)$ satisfy a polynomial equation $t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n = 0$, where $\alpha_i \in A$. Then $\alpha^n$ is divisible by $\beta$. Since $A$ is factorial, each irreducible divisor of $\beta$ divides $\alpha$, that is, $\alpha/\beta \in A$. □

Claim 8.22. *A Noetherian ring without zero divisors is factorial iff all its irreducible elements are prime.*

Proof. In a Noetherian ring, any element $f$ is a finite product of irreducible elements: in the contrary case $f$ can written as $f = f_1 g_1$, where $f_1$ is reducible and can be written as $f = f_2 g_2$ an so on *infinitely* many times producing an infinite chain of strictly increasing ideals $(f) \subset (f_1) \subset (f_2) \subset (f_2) \subset \ldots$. Further, if there are no zero divisors and all irreducible elements are prime, then two irreducible factorizations $\prod q_i = \prod q'_j$ have the same number of factors and satisfy $q_i = s_i q'_i$ for some invertible $s_i$ (after appropriate renumbering). Indeed, since prime $q'_1$ divides $\prod q_i$ it divides some $q_i$, say $q_1$. So, $q_1 = s_1 q'_1$, where $s_1$ is invertible, because $q_1$ is irreducible. Now we have $q'_1 \left( s_1 \prod\limits_{i \geqslant 2} q_i - \prod\limits_{j \geqslant 2} q'_j \right) = 0$, which implies $s_1 \prod\limits_{i \geqslant 2} q_i = \prod\limits_{j \geqslant 2} q'_j$, and we can replace $q_2$ by $s_1 q_2$ and use induction over the number of factors.

It remains to note that in factorial ring all irreducible elements are prime: if $ab = pq$, where $q$ is irreducible, then irreducible factorization of either $a$ or $b$ should contain an element $sq$ with invertible $s$. □

GREATEST COMMON DIVISOR. Let $A$ be a factorial ring and $a_1, a_2 \in A$ have the prime factorizations:

$$a_1 = q_1 \cdots q_s q'_{s+1} \cdots q'_m \,, \quad a_2 = q_1 \cdots q_s q'_{s+1} \cdots q'_n \,,$$

where no $q'_i$, $q'_j$ are associated (the case $s = 0$, without any $q$'s, is also possible). The product $q_1 \cdots q_s$ (or 1, if $s = 0$) is called *the greatest common divisor* of $a_1$, $a_2$ and denoted by $GCD(a_1, a_2)$. Note that $GCD(a_1, a_2)$ is defined up to invertible factor. Inductively, $GCD(a_1, a_2, \ldots, a_n) = GCD\,(GCD(a_1, a_2, \ldots, a_{n-1}), a_n)$. Given a polynomial $f = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \in A[x]$, then $GCD(a_1, a_2, \ldots, a_n)$ is called *a content* of $f$ and is denoted by $cont(f)$.

Claim 8.23. $cont(fg) = cont(f)cont(g)$ *for any* $f, g \in A[x]$.

Proof. It is enough to check that $cont(fg) = 1$, if $cont(f) = cont(g) = 1$. If all the coefficients of $fg$ are divisible by some prime $p \in A$, then $fg \pmod p = 0$ in the ring $(A/pA)[x]$, which has no zero divisors, because $p$ is prime. So, either $f \pmod p = 0$ or $g \pmod p = 0$. □

Claim 8.24. *If $A$ is factorial, then $A[x]$ is factorial as well.*

Proof. Let $k = Q(A)$ be the quotient field. By Claim 8.22, it is enough to show that any irreducible $f \in A[x]$ remains to be irreducible inside the factorial ring $k[x]$. Let $f = gh$ in $k[x]$. We can write $g(x) = a^{-1}g'(x)$, $h(x) = b^{-1}h'(x)$ for some $a, b \in A$ and $g', h' \in A[x]$ such that $cont(g') = cont(h') = 1$. Now $ab\,f = g'h'$, where $cont(g'h') = 1$ by Claim 8.23 and $cont(f) = 1$, because $f$ is irreducible in $A[x]$. Hence. $ab$ is invertible and $h'' = (ab)^{-1}h' \in A[x]$. This leads to the decomposition $f = h''g'$ inside $A[x]$. □

Corollary 8.25. *If $A$ is factorial, then $A[x_1, x_2, \ldots, x_n]$ is factorial (in particular, normal).* □

Exercice 8.26. Let $k$ be an algebraically closed field of any characteristic, $X \subset \mathbb{A}_n(k)$ be an algebraic hypersurface given by a polynomial equation $f(x_1, x_2, \ldots, x_n) = 0$, where $f \in k[x_1, x_2, \ldots, x_n]$, and let $g(x) \in k[x_1, x_2, \ldots, x_n]$ vanish at any point of $X$. Show that $g$ is divisible by any irreducible factor of $f$

HINT. Since $k[x_1, x_2, \ldots, x_n]$ is factorial, the result follows from Hilbert's Nullstellensatz

RESULTANT SYSTEMS. We fix a collection of $m$ degrees $d_1, d_2, \ldots, d_m$ and write $\mathscr{S}_d = \mathbb{P}(S^d V^*)$ for the space of hypersurfaces of degree $d$ in $\mathbb{P}_n = \mathbb{P}(V)$. Let $\mathscr{R} \subset \mathscr{S}_{d_1} \times \mathscr{S}_{d_2} \times \cdots \times \mathscr{S}_{d_m}$ be a set of all hypersurface collections $S_1, S_2, \ldots, S_m \subset \mathbb{P}_n$ such that $\bigcap S_\nu \neq \varnothing$. Then $\mathscr{R}$ is an *algebraic variety*, i. e. can be described by a finite system of multi-homogeneous polynomial equations on the coefficients of forms $(f_1, f_2, \ldots, f_m) \in S^{d_1}V^* \times \cdots \times S^{d_n}V^*$ defining the hypersurfaces $S_1, S_2, \ldots, S_m$. This equation system depends only on $n$, $d_1, d_2, \ldots, d_m$ and is called *a resultant system*. Indeed, consider an ideal $I \subset k[\,x_0, x_1, \ldots, x_n\,]$ generated by $f_\nu$. Then $\bigcap S_\nu \subset \mathbb{P}(V)$ is empty $\iff$ $V(I) \subset \mathbb{A}(V)$ either is empty or coincides with the origin $O \in \mathbb{A}(V)$. In the both cases each $x_i$ vanishes along $V(I)$, i. e. by Hilbert's Nullstellensatz $x_i^m \in I$ for some $m$, that is $S^d V^* \subset I \;\forall\, d \gg 0$. Since $V(x_0^m,\, x_1^m,\, \ldots\,,\, x_n^m) = \{O\}$ this condition is also sufficient. So, $\bigcap S_\nu = \varnothing$ iff $k$-linear map:

$$\mu_d \;:\; S^{d-d_0}V^* \oplus S^{d-d_1}V^* \oplus \cdots \oplus S^{d-d_n}V^* \xrightarrow{\;(g_0, g_1, \ldots, g_n) \mapsto \sum g_\nu f_\nu\;} S^d \tag{26}$$

is non surjective $\forall\, d \gg 0$. In terms of the standard monomial bases, $\mu_d$ is presented by a matrix whose entries are linear forms in the coefficients of $f_\nu$. Since for $d \gg 0$ the dimension of the left side in (26) becames greater then the right one[8], $\mathscr{R}$ coincides with the zero set of all $d \times d$ - minors of all $\mu_d$ with $d$ large enough. By Hilbert's base theorem, this infinite equation system is equivalent to some finite subsystem. Say, we will see in

[8] the leading terms of their expansions as polynomials in $d$ are $md^n/n!$ and $d^n/n!$ respectively

Example 8.28 that for $n=1$, $m=2$ the smallest $d$ producing a non trivial restriction is $d=d_0+d_1-1$, where $\mu_d$ becomes a square matrix; in this case $\mathscr{R}$ is a hypersurface given by just one equation $\det \mu_{d_0+d_1-1}=0$.

Example 8.27: projection $\mathbb{P}_m \times \mathbb{A}^n \xrightarrow{\pi} \mathbb{A}^n$ sends algebraic varieties to algebraic varieties, i. e. as soon as $X = \{\,(q,p) \in \mathbb{P}_m \times \mathbb{A}^n \mid f_\nu(q,p)=0\,\}$ is given by polynomial equations[9] $f_\nu(t,x)=0$ its projection onto $\mathbb{A}^n$ is also a zero set of some system of polynomials. Indeed, consider $f_\nu$ as homogeneous polynomials in $t$ with the coefficients in $k[x_1,x_2,\ldots,x_n]$. Then the image $\pi(X)\subset\mathbb{A}^n$ consists of all $p$ such that the homogeneous in $t$ polynomials $f_\nu(t,p)$ have a common zero on $\mathbb{P}_m$. As we have seen before, this means that their coefficients, which are some polynomials in $p$, satisfy the system of resultant equations.

Example 8.28: resultant of two binary forms. If $k$ is algebraically closed, then each polynomial $f(t)=a_0\,t^m+a_1\,t^{m-1}+\cdots+a_{m-1}\,t+a_m$ can be factorized as $f(t)=a_0\prod(t-\vartheta_\nu)=a_m\prod(1-\vartheta_\nu^{-1}t)$, where $\vartheta_1,\vartheta_2,\ldots,\vartheta_m$ are all its roots. In homogeneous world, each degree $d$ homogeneous polynomial

$$A(t_0,t_1)=a_0\,t_1^d+a_1\,t_0\,t_1^{d-1}+a_2\,t_0^2\,t_1^{d-2}+\;\cdots\;+a_{d-1}\,t_0^{d-1}\,t_1+a_d\,t_0^d$$

has similar decomposition $A(t_0,t_1)=\prod\limits_{i=0}^{d}(\alpha_i''t_0-\alpha_i't_1)=\prod\limits_{i=0}^{d}\det\begin{pmatrix}t_0 & t_1\\ \alpha_i' & \alpha_i''\end{pmatrix}$, which means that $A$ vanishes at $d$ points $\alpha_1,\alpha_2,\ldots,\alpha_d\in\mathbb{P}_1$ with homogeneous coordinates $\alpha_i=(\alpha_i':\alpha_i')$. In particular, each coefficient $a_i$, of $A(t)$, is expressed as bihomogeneous degree $(i,d-i)$ polynomial in $(\alpha',\alpha'')$:

$$a_i=(-1)^{d-i}\sigma_i(\alpha',\alpha'')\,,\quad\text{where}\quad \sigma_i(\alpha',\alpha'')=\sum_{\#I=i}\Big(\prod_{i\in I}\alpha_i'\cdot\prod_{j\notin I}\alpha_j''\Big)$$

(here $I$ runs through all increasing length $i$ subsets in $\{1,2,\ldots,d\}$ and $\sigma_i$ is a *bi*homogeneous version of the $i$-th elementary symmetric function).

Now, let us fix two degrees $m,n\in\mathbb{N}$ and consider a polynomial ring $k[\alpha',\alpha'',\beta',\beta'']$ in four collections of variables $\alpha'=(\alpha_1',\alpha_2',\ldots,\alpha_n')$, $\alpha''=(\alpha_1'',\alpha_2'',\ldots,\alpha_n'')$, $\beta'=(\beta_1',\beta_2',\ldots,\beta_m')$, $\beta''=(\beta_1'',\beta_2'',\ldots,\beta_m'')$ Then the product

$$R_{AB}\overset{\text{def}}{=}\prod_{i,j}\big(\alpha_i'\beta_j''-\alpha_i''\beta_j'\big)=\prod_{j=1}^{n}A(\beta_j)=(-1)^{mn}\prod_{i=1}^{m}B(\alpha_i)\,,$$

vanishes iff two homogeneous binary forms $A(t_0,t_1)=\sum\limits_{i=0}^{n}a_i\,t_0^i\,t_1^{n-i}$ and $B(t_0,t_1)=\sum\limits_{j=0}^{m}b_j\,t_0^j\,t_1^{m-j}$ (whose coefficients $a_i=(-1)^{n-i}\sigma_i(\alpha',\alpha'')$, $b_j=(-1)^{m-j}\sigma_j(\beta',\beta'')$ have a common root. Clearly, $R_{A,B}$ is bihomogeneous of bidegree $(mn,mn)$ in $(\alpha,\beta)$ and may be expressed in terms of the coefficients of $A$, $B$. This expression is called *a resultant* of the polynomials $A(t_0,t_1)$, $B(t_0,t_1)$ and generates the ideal of all resultant relations for two binary forms. More precisely, $R_{A.B}$ up to a scalar factor coincides with *the Silvester determinant*

$$\det\underbrace{\left.\begin{pmatrix}
a_0 & a_1 & \ldots & a_n & & & \\
 & a_0 & a_1 & \ldots & a_n & & \\
 & & \ddots & \ddots & & \ddots & \\
 & & & a_0 & a_1 & \ldots & a_n \\
b_0 & b_1 & \ldots & b_m & & & \\
 & b_0 & b_1 & \ldots & b_m & & \\
 & & \ddots & \ddots & & \ddots & \\
 & & & b_0 & b_1 & \ldots & b_m
\end{pmatrix}\right\}\begin{matrix}m\\ \\ \\ \\ \\ \\ \\ n\end{matrix}}_{m+n}$$

Indeed, consider a vector space $U$ with a basis $\{t_0,t_1\}$ and a linear map $S^{m-1}U\oplus S^{n-1}U\xrightarrow{M_{A,B}}S^{m+n-1}U$ which sends a pair of polynomials $(h_1(t),h_2(t))$ to $A(t)h_1(t)+B(t)h_2(t)$ as in 26. The Silvester matrix is transpose to the matrix of $M_{A,B}$ in the standard monomial bases. If a point $(\alpha,\beta)$ lies on the quadric $\alpha_i'\beta_j''-\alpha_i''\beta_j'=0$, then $(\alpha_i''t_0-\alpha_i't_1)=(\beta_i''t_0-\beta_i't_1)$ up to a scalar factor. This linear form divides $A(t)$, $B(t)$ and any polynomial $A(t)h_1(t)+B(t)h_2(t)$. Hence, $\operatorname{im}M_{A,B}\neq S^{m+n-1}U$. So, the Silvester determinant vanishes along each quadric $\alpha_i'\beta_j''-\alpha_i''\beta_j'=0$ and, by Hilbert's Nullstellensatz, it is divisible by $R_{A,B}$. The quotient has to be a constant, because the both polynomials are bihomogeneous of the same bidegree $(mn,mn)$ in $(\alpha,\beta)$. Moreover, since the Silvester determinant vanishes as soon $A(t)$ and $B(t)$ are not coprime, $R_{AB}$ spans the ideal of all resultant relations — so, it is principal in the case of two binary forms.

Example 8.29: Elimination technique. Let $C_1$, $C_2$ be two plane curves of degrees $m$ and $n$ given by equations $F(x)=0$ and $G(x)=0$ in $x=(x_0:x_1:x_2)$. Consider $F$, $G$ as (non homogeneous) polynomials in $x_0$ with the coefficients in

[9] homogeneous in $t=(t_1,t_2,\ldots,t_m)\in\mathbb{P}_m$

$k(x_1, x_2)$ and take their resultant[10] $R_{F,G}(x_1, x_2) \in k[x_1, x_2]$. If it is identically zero, then $F$ and $G$ have a common divisor in $k(x_1, x_2)[x_0]$.

Exercice 8.30. Deduce from the Gauss – Kronecker – Dedekind lemma that this common divisor can be taken with the coefficients in $k[x_1, x_2]$.

So, if $R \equiv 0$, then $C_1$ and $C_2$ have a common component. If $R \not\equiv 0$, then $(x_1, x_2)$-coordinates of any intersection point $p \in C_1 \cap C_2$ have to satisfy the resultant equation $R_{F,G}(x_1, x_2) = 0$ which is homogeneous of degree $mn$. So, the curves have either a common component or at most $mn$ intersection points, which may be found by solving a homogeneous polynomial equation in $x_1, x_2$ only. These procedure is called *an elimination of a variable*.

[10] resultant of non-homogeneous polynomials $F(x_0)$ and $G(x_0)$ is defined as the resultant of $t_0^n F(t_1/t_0)$ and $t_0^m G(t_1/t_0)$